réf : FGN

Polynômes irréductibles

Leçons 123, 125, 141, 144

Sur $\mathbb{F}_q$:

Définition : On définit la fonction de Möbius μ par

$$\begin{cases} \mu(1) = 1 \\ \mu(n) = 0 \text{ si } n \text{ est divisible par le carré d'un nombre premier} \\ \mu(p_1 \cdots p_r) = (-1)^r \text{ si les } p_i \text{ sont premiers deux à deux distincts.} \end{cases}$$

Proposition : On a $\sum_{d \mid n} \mu(d) = \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{si } n > 1 \end{cases}$

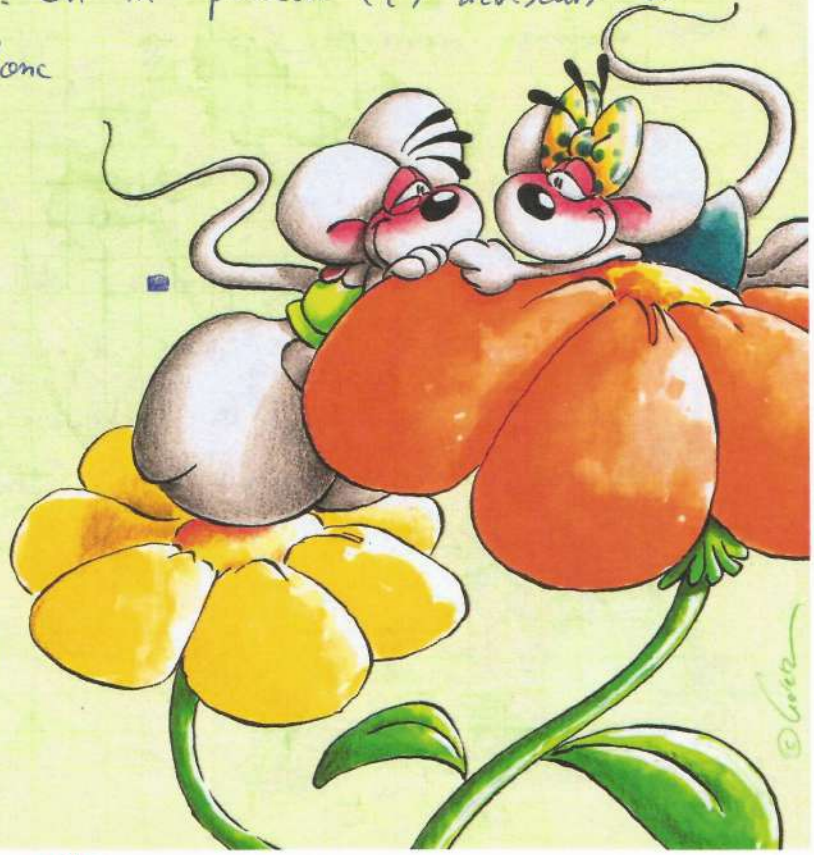
Preuve proposition :

Posons $S(n) = \sum_{d \mid n} \mu(d)$. Calculons maintenant $S(n)$ pour $n \in \mathbb{N}^*$:

On a tout d'abord $S(1) = 1$. Soit $n \geq 2$ et soit sa décomposition en facteurs premiers $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ où $p_1, \dots, p_k$ sont des nombres premiers distincts et $\alpha_1, \dots, \alpha_p$ des entiers strictement positifs.

Les seuls diviseurs d de n pour lesquels $\mu(d)$ est non nul sont les produits de nombres premiers distincts pris parmi $p_1, \dots, p_k$. Pour un tel diviseur, on a $\mu(d) = (-1)^i$ où i est le nombre de diviseurs premiers de d. On n possède $\binom{k}{i}$ diviseurs d à un i fixé. On a donc

$$\begin{aligned} S(n) &= \sum_{i=0}^{k} \binom{k}{i} (-1)^i \\ &= (1-1)^k \\ &= 0. \end{aligned}$$



Proposition :

Soit $f : \mathbb{N}^* \longrightarrow \mathbb{R}$. Si on pose $g : \mathbb{N}^* \longrightarrow \mathbb{R}$, $n \longmapsto \sum_{d \mid n} f(d)$

alors $\forall n \geq 1$, $f(n) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) g(d) = \sum_{d \mid n} \mu(d)\, g\left(\frac{n}{d}\right)$

Preuve :

Soit $n \geq 1$. On a $\sum_{d \mid n} \mu(d)\, g\left(\frac{n}{d}\right) = \sum_{d \mid n} \mu(d) \cdot \left(\sum_{d' \mid \frac{n}{d}} f(d')\right)$

$= \sum_{d' \mid n} f(d') \cdot \left(\sum_{d \mid \frac{n}{d'}} \mu(d)\right)$

$= f(n)$ par la proposition précédente. ∎

Proposition :

Soit $\mathbb{F}_q$ corps fini de cardinal q, q puissance d'un nbre premier.

$\forall n \in \mathbb{N}^*$, il existe un polynôme irréductible sur $\mathbb{F}_q$ de degré n.

Le nombre de tels polynômes est équivalent à $\frac{q^n}{n}$ pour $n \to +\infty$.

Preuve :

Soit $n \in \mathbb{N}^*$, on note $A(n,q)$ l'ensemble des polynômes de $\mathbb{F}_q[X]$ irréductibles unitaires de degré n et $I(n,q) = \mathrm{Card}(A(n,q))$.

- Nous voulons montrer $X^{q^n} - X = \prod_{d \mid n} \prod_{P \in A(d,q)} P = \prod_{\{P \in \mathbb{F}_q[X] ;\, d(P) \mid n \text{ et } P \in A(\deg P, q)\}} P$

Comme $\mathbb{F}_q[X]$ est factoriel, on peut écrire la décomposition en facteurs premiers de $X^{q^n} - X$ et comme les racines dans $\mathbb{F}_{q^n}$ de $X^{q^n} - X$ sont simples, tout les facteurs irréductibles sont différents et vont apparaître une fois dans la décomposition de $X^{q^n} - X$.

$$X^{q^n} - X = \prod_{\{Q \text{ facteur irréductible de } X^{q^n} - X\}} Q.$$

On veut donc montrer que (par double inclusion)

$A = \{ Q \text{ facteur inéductible de } X^{q^n} - X \} = \{ P \in \mathbb{F}_q[X] ;\ d^\circ P \mid n \text{ et } P \in A(d^\circ P, q) \} = B$

▶ Mq B C A

Soit $P \in B$. Nous allons montrer que P divise $X^{q^n} - X$.

Soit $K = \mathbb{F}_q[X]/(P) = \mathbb{F}_q(x)$ un corps de rupture de P, où x est racine de P (comme P est inéductible, ce corps de rupture est unique à isomorphisme de $\mathbb{F}_q$ algèbres près). Comme P est inéductible à coefficients dans $\mathbb{F}_q$, unitaire et annulateur pour x, alors P est le polynôme minimal de x. On a $[K : \mathbb{F}_q] = d^\circ(P) = d$. Par unicité des corps finis, on a donc K isomorphe à $\mathbb{F}_{q^d}$.

On sait que $\mathbb{F}_{q^d} = \{ \text{racines de } X^{q^d} - X \}$ (en effet : Soit $a \in \mathbb{F}_{q^d}^*$ alors $a^{q^d - 1} - 1 = 0$ et donc $a^{q^d} = a$. Ainsi $\mathbb{F}_{q^d}^* \subset \{ \text{racines de } X^{q^d} - X \}$. C'est aussi le cas de 0 donc $\mathbb{F}_{q^d} \subset \{ \text{racines de } X^{q^d} - X \}$. Vu que $\operatorname{card} \{ \text{racines de } X^{q^d} - X \} \leq q^d$, on a égalité.)

On a donc en particulier $x^{q^d} = x$. Comme $d \mid n$, on a

$$x^{q^n} = \underbrace{(\cdots((x^{q^d})^{q^d})\cdots)^{q^d}}_{n/d \text{ fois}} = \underbrace{(\cdots((x^{q^d})^{q^d})\cdots)^{q^d}}_{n/d - 1 \text{ fois}} = \cdots = x$$

et ainsi x racine de $X^{q^n} - X$. On applique ce même raisonnement à toutes les racines de P, et on obtient $P \mid X^{q^n} - X$. De plus P inéductible, d'où $P \in A$.

▶ Mq $A \subset B$

Soit $P \in A$. Montrons $d^\circ P$ divise n.

Soit $d = d^\circ(P)$. Le polynôme $X^{q^n} - X$ est scindé sur $\mathbb{F}_{q^n}$. Soit x une racine de P dans $\mathbb{F}_{q^n}$. On note $K = \mathbb{F}_q(x)$. On a donc $n = [\mathbb{F}_{q^n} : \mathbb{F}_q] = [\mathbb{F}_{q^n} : K] \times [K : \mathbb{F}_q]$

$= [\mathbb{F}_{q^n} : K] \times d$

Ainsi, $d \mid n$. De plus, vu que P est irréductible, on a aussi $P \in A(d, q)$ et donc $P \in B$.

- Nous voulons montrer que $\sum_{d \mid n} d \cdot I(d, q) = q^n$.

On sait par ce qui précède que $X^{q^n} - X = \prod_{d \mid n} \prod_{P \in A(d,q)} P$

et en regardant les degrés, on obtient $\sum_{d \mid n} d \cdot I(d, q) = q^n$.

- Nous voulons montrer que $I(n, q) = \frac{1}{n} \sum_{d \mid n} \mu\left(\frac{n}{d}\right) q^d$.

Pour cela on utilise la formule d'inversion de Möbius appliquée à la fonction $n \mapsto n \cdot I(n, q)$:

$$n \cdot I(n,q) = \sum_{d \mid n} \mu(d) \cdot \sum_{d' \mid \frac{n}{d}} d' \cdot I(d', q)$$

$$= \sum_{d \mid n} \mu(d)\, q^{n/d} \quad \text{par le point précédent}$$

$$= \sum_{d \mid n} \mu\left(\frac{n}{d}\right) \cdot q^d$$

• Montrons que $I(n,q) \underset{n\to+\infty}{\sim} \frac{q^n}{n}$:

On a $I(n,q) = \frac{q^n + r_n}{n}$ avec $r_n = \sum_{\substack{d|n \\ d<n}} \mu\left(\frac{n}{d}\right) . q^d$

On majore r_n :

$$|r_n| \leq \sum_{d=1}^{E\left(\frac{n}{2}\right)} q^d = q \cdot \frac{q^{E\left(\frac{n}{2}\right)} - 1}{q-1}$$

$$\leq \frac{q^{E\left(\frac{n}{2}\right)+1}}{q-1}$$

Ainsi en divisant cette inégalité par q^n, on a que r_n est négligeable devant q^n quand $n \to +\infty$.

On obtient ainsi l'équivalent $I(n,q) \underset{n\to+\infty}{\sim} \frac{q^n}{n}$. ■